Summary Statement—Glenn Podonsky—Testimony—June 13, 2000

I appreciate the opportunity to appear before this committee to discuss our April inspection of unclassified cyber security systems at the DOE Headquarters. As you know, the Office of Independent Oversight and Performance Assurance provides the Secretary of Energy with an independent view of the effectiveness of safeguards and security, emergency management, and cyber security policies and programs throughout the DOE complex.

In the past, DOE sites often focused on making information easily available and computer systems easy to use, which frequently led to cyber security receiving a low priority. Also, DOE policy was not always followed, which allowed implementation of computer systems in ways that did not provide for effective security. Particularly disturbing was the situation in Los Alamos in 1994 when my office pointed out that the classified network had connections to the unclassified network, posing the risk that an authorized user could download large quantities of classified information to an unclassified computer with little chance of detection.

Over the past 15 years, the DOE Headquarters has often received less than satisfactory ratings in many areas, including cyber security. Until Secretary Richardson's involvement, the program offices were in some cases unwilling to commit resources to enhance security. Recent results, however, have been more positive. A number of cyber security upgrades and other initiatives have been completed or are underway.

The results of our inspection indicate that important deficiencies still need to be addressed. Many program offices have cyber security programs that would be considered effective if they were not connected to less effective networks. Generally, the main Headquarters firewall is effective; however, several Web servers managed by individual program offices are located completely outside the firewall boundary. Most were found to be vulnerable to hacking and some have vulnerabilities that could allow any Internet user to gain system administrator-level privileges and subsequently deface or shut down the Web site. Headquarters has not developed overall cyber security procedures or minimum requirements for each network segment on the network.

The fragmented management systems and practices currently in place are a root cause of many identified weaknesses. While the Chief Information Officer has attempted to address many of these weaknesses, the effectiveness of these initiatives has been limited due to the lack of real and perceived authority. This fragmentation results in part from weaknesses in policy, which does not address the unique situation at Headquarters or establish overall responsibilities and authorities.

My office is continually expanding its ability to conduct network performance tests using tools we have acquired or developed. We currently have an extensive cyber security laboratory dedicated to testing cyber security features. We also conduct regular inspections of cyber security systems at DOE sites. We will conduct an inspection of "classified" cyber security at the DOE Headquarters in July 2000 in conjunction with a comprehensive inspection of safeguards and security policies and programs. We also will continue to follow-up and work closely with the Office of Security and Emergency Operations as they work to clarify and enhance cyber security policy and guidance.

Although much work remains, it is clear that a positive trend in unclassified cyber security has been established at DOE Headquarters. Much of the recent improvement can be attributed to the attention and efforts of the Secretary of Energy and the Chief Information Officer.